

DEMOCRACIA DIGITAL: OS RUMOS DA REGULAMENTAÇÃO LEGISLATIVA NO ORDENAMENTO JURÍDICO BRASILEIRO

Bruna Pinotti Garcia¹ e Guilherme Domingos de Luca²

Resumo

Os rumos da democracia na *Web* dependem da postura legislativa a respeito dos conflitos nela estabelecidos. Utilizando pesquisa bibliográfica e documental, parte-se do estudo dos limites ao exercício da liberdade na *Internet*, que se excedidos caracterizam ato ilícito. O artigo efetua um estudo comparativo entre o Projeto de Lei n. 84/1999 e o n. 2126/2011, concluindo que o segundo atende melhor às necessidades da democracia digital.

Palavras-chave

Democracia digital. Conflitos na *Web*. Atos ilícitos na *Internet*. Projeto de Lei n. 84/1999. Projeto de Lei n. 2126/2011.

Abstract

The direction of Web democracy depends on the legislative position regarding the conflicts therein. Using bibliographical and documentary survey, it begins of the limits to the exercise of

¹ Advogada. Mestranda em Direito do Centro Universitário Eurípides de Marília – UNIVEM, bolsista CAPES – Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (modalidade 1). Membro do Núcleo de Estudos e Pesquisas em Direito e *Internet*.

² Graduando em Direito do Centro Universitário Eurípides de Marília – UNIVEM, bolsista PIBIC – Programa Institucional de Bolsas de Iniciação Científica. Membro do Núcleo de Estudos e Pesquisas em Direito e *Internet*.

freedom on the Internet study, which exceeded characterize unlawful act. The article makes a comparative study of the Draft Law n. 84/1999 and n. 2126/2011, concluding that the second best meets the needs of digital democracy.

Keywords

Digital democracy. Conflicts on the Web. Unlawful act on the Internet. Draft Law n. 84/1999. Draft Law n. 2126/2011.

1 Introdução

Cada dia mais a *Internet* se faz presente nas relações sociojurídicas em geral. Ela proporciona um ambiente virtualizado, o que não significa que as atitudes neste praticadas não produzam efeitos tangíveis. Com efeito, nota-se uma vulnerabilidade social decorrente dos ilícitos cometidos em face do uso indevido ou abusivo desta ferramenta.

Por isso, este ambiente virtual, que já foi considerado por alguns um espaço sem dono, livre de qualquer normatização, tem sido regulamentado pelo Estado, tanto sob o aspecto legiferante quanto sob o judicante, isto é, legislando-se a respeito e solucionando conflitos pela via judicial.

O Poder Judiciário tem o dever de prestar a tutela jurisdicional em cada conflito que é perante ele invocado, independentemente de disciplina legal específica. Logo, todo e qualquer litígio envolvendo a questão informática pode ser levado ao Judiciário.

Há quem considere a ausência de uma norma jurídica específica em regular certos conflitos oriundos da *Internet* como a responsável pelos crescentes litígios. Em via oposta, corrente entende que as Leis materiais e processuais vigentes são capazes de proteger o ciberespaço, estando certo o aplicador da norma em valer-se, inclusive, de uma postura Neopositivista, utilizando a Nova Hermenêutica Constitucional como instrumento jurídico de solução das controvérsias na rede.

O exercício da liberdade e de qualquer outro direito na *Web* se sujeita a limites: o excesso no exercício de tais direitos caracteriza a

prática de ato ilícito *lato sensu*. Logo, não é possível afastar totalmente a ingerência estatal, mas apenas se pode buscar que ela respeite ao máximo a preservação da democracia digital.

Justifica-se a pesquisa porque há muito o que se compreender a respeito da regulamentação de conflitos na *Web*, no sentido de que alguma das posturas possíveis é a mais adequada sob o aspecto da garantia da democracia digital. Sem um debate ativo no âmbito acadêmico quanto a tais questões é possível que seja criado um cenário jurídico policalesco na *Internet*, no qual ela perca sua essência, qual seja o caráter libertário e democrático.

Considerado este contexto, busca-se, como objetivo geral, traçar um panorama a respeito da postura legislativa estatal, efetuando estudo comparativo de dois Projetos de Lei, o n. 84/1999 e o n. 2126/2011, os quais abordam de maneira substancialmente diversa a questão da solução de conflitos que se estabelecem na *Internet*. A título de objetivos específicos, pretende-se: compreender os limites jurídicos e filosóficos ao exercício da liberdade no ciberespaço, estudar os conflitos que se estabelecem na *Web* e a forma como estes permitem a caracterização de atos ilícitos (cíveis e criminais), pontuar a postura estatal que vem sendo assumida no âmbito do direito eletrônico e estudar dois dos projetos de lei que tramitam a respeito da questão. Ao final, pretende-se concluir qual dos sistemas propostos, em linhas gerais, é o mais apto sob o aspecto da efetivação da democracia digital.

Para tanto, adota-se pesquisa bibliográfica e documental, efetuando uma revisão de literatura a respeito de temas como os limites ao exercício da liberdade e a prática de atos ilícitos no ciberespaço, para então serem levantados os projetos de lei mais antagônicos a respeito da intervenção estatal na *Internet*.

2 Limites da liberdade e de seu exercício no ciberespaço

Para entender os limites a que o usuário da rede se sujeita ao utilizar a *Internet*, é importante destacar o que vem a ser liberdade,

para a partir daí poder traçar o é lícito ou não em seu exercício. Desta forma, cumpre-se aqui demonstrar os conceitos de liberdade segundo o senso comum, a filosofia e, por fim, o Direito.

Pelo senso comum, que é o conhecimento que o homem adquire da tradição que herdou dos antepassados, ao qual se acrescentam resultados de experiências vividas, entende-se que a liberdade é o estado em que a pessoa ou coisa encontra-se livre de qualquer limite, coação, constrangimento ou imposição de outra parte, podendo agir por meio de sua livre consciência. Ferreira³ assim conceitua:

Li.ber.da.de sf. 1. Faculdade de cada um se decidir ou agir segundo a própria determinação. 2. Estado ou condição de homem livre. 3. Confiança, intimidade (às vezes abusiva). Liberdade condicional. Jur. Liberdade com algumas condições restritivas, que se dá a certos condenados, antes do fim da pena.

No conceito do Dicionário Aurélio, percebe-se que a liberdade do senso comum se define quando o conteúdo da liberdade é apenas um fazer, uma faculdade de agir ou não. Por outro lado, o item 3 do conceito já expõe que o exercício da liberdade pode ser abusivo, aspecto que sai um pouco da ideia de senso comum para se aproximar de um aspecto filosófico da liberdade.

Na filosofia, a liberdade possui um conceito muito mais amplo que o senso comum coletivo, envolvendo uma forma negativa, caracterizada pela ausência de submissão, servidão e determinação, o que qualifica a independência humana; bem como uma positiva, referindo-se à espontaneidade do sujeito pensante. Aranha e Martins⁴ entendem que, para a liberdade ser alcançada, deve-se atingir uma condição:

A liberdade de cada um é limitada unicamente pela liberdade dos demais. O que se esquece é que nem sempre a liberdade de escolha é tão livre quanto se apregoa, sobretudo nas sociedades em que predominam privilégios para poucos, delimitando o campo de ação da maioria. Sabemos que a vida moral só é possível com ação baseada na cooperação, na reciprocidade e no desenvolvimento da responsabilidade e do compromisso. Só assim torna-se viável a efetiva liberdade de cada um. Nesse sentido, o outro não é o limite da nossa liberdade, mas a condição para atingi-la.

³ FERREIRA, Aurélio Buarque de Holanda. **Miniaurélio**: o minidicionário da língua portuguesa. Curitiba: Positivo, 2004, p. 525.

⁴ ARANHA, Maria Lúcia de Arruda; MARTINS, Maria Helena Pires. **Filosofando**: Introdução à Filosofia. 3 ed. São Paulo: Moderna, 2003, p. 322.

Percebe-se, no conceito filosófico, que para o adequado exercício da liberdade há limitações a ela inerentes. Tradicionalmente, na filosofia, a condição de exercício de qualquer direito individual, para ser considerado virtuoso, é o respeito ao equilíbrio, ao meio-termo, de modo a não prejudicar terceiros.

Aristóteles⁵ considerou que está na natureza das virtudes serem destruídas pela deficiência e pelo excesso, sendo necessário buscar o meio-termo. Já Kant⁶ determinou a lei fundamental da razão pura prática com base em dois fundamentos: o primeiro é o de que, sendo possível a determinação da vontade com base em uma vontade livre de inclinações, é preciso encontrar uma lei apta para realizar tal determinação; e o segundo é o de que existe uma lei moral da qual temos consciência imediata, que não pode ser ultrapassada por nenhuma condição sensível. A lei fundamental da razão pura prática em Kant⁷ se resume no seguinte postulado: "age de tal modo que a máxima de tua vontade possa valer-te sempre como princípio de uma legislação universal". Nos ensinamentos de ambos os filósofos resta clara a existência de limitações ao exercício de qualquer direito, de modo a respeitar os interesses de terceiros e da sociedade.

Já o ordenamento jurídico traz a liberdade como um direito fundamental do homem. Trata-se do estado em que a pessoa encontra-se livre de limites e coações, desde que aja de forma lícita e de acordo com os princípios éticos da sociedade, os quais se encontram consubstanciados em normas.

A liberdade prevista no ordenamento jurídico é protegida pela Constituição Federal brasileira, promulgada no ano de 1988, na qual se garante a liberdade como: a manifestação de pensamento (artigo 5º, IV e V); de consciência, crença e culto (artigo 5º, VI a VIII); de atividade intelectual, artística, científica ou de comunicação, com indenização em caso de danos (artigo 5º, IX e

⁵ ARISTÓTELES. **Ética a Nicômaco**. Tradução Pietro Nasseti. São Paulo: Martin Claret, 2006, p. 42.

⁶ KANT, Immanuel. **Crítica da Razão Prática**. Tradução Paulo Barrera. São Paulo: Ícone, 2005, p. 30-31.

⁷ Idem. *Ibidem*, p. 32.

X); de profissão (artigo 5º, XIII); de informação (artigo 5º, XIV e XXXIII); de locomoção (artigo 5º, XV e LXI); entre outras. Entendem, assim, Motta e Barchet⁸:

Um dos mais amplos direitos fundamentais consagrados na Constituição, o direito à liberdade de manifestação do pensamento, respeitados os demais direitos fundamentais, não segue qualquer norma de forma ou de fundo. Qualquer um pode manifestar seu pensamento sobre qualquer coisa por qualquer meio de expressão, desde que se identifique ao manifestar-se, como precaução indispensável contra declarações levianas ou infundadas, as quais podem ensejar responsabilização.

Silva⁹ aponta que a liberdade de pensamento, também chamada de liberdade de opinião, é considerada pela doutrina como a liberdade primária, eis que é ponto de partida de todas as outras, e deve ser entendida como a liberdade da pessoa adotar determinada atitude intelectual ou não, de tomar a opinião pública que crê verdadeira. A partir daí, no entender de Silva¹⁰, tem-se a liberdade de expressão, que pode ser vista sob diversos enfoques, como o da liberdade de comunicação, ou liberdade de informação, que consiste em um conjunto de direitos, formas, processos e veículos que viabilizam a coordenação livre da criação, expressão e difusão da informação e do pensamento. Como todos os direitos, aqueles inerentes às dimensões da liberdade sofrem limitações, por exemplo, pela privacidade, pela personalidade e pela propriedade intelectual.

No tocante à liberdade a ser exercida na *Internet*, também estão presentes elementos limitativos. Em que pese a postura inicial de que na rede mundial de computadores não haveria qualquer sujeição ao Direito, com o tempo se percebeu que os reflexos dos atos ali praticados na realidade eram extremamente relevantes. Com efeito, se mostrou necessária a aplicação da Moral e do Direito enquanto limitadores do exercício da liberdade.

Um fator que muito influenciou este contexto foi o espaço que a *Internet* passou a ocupar na sociedade. Cada vez mais ela se torna

⁸ MOTTA, Sylvio; BARCHET, Gustavo. **Curso de Direito Constitucional**. Rio de Janeiro: Elsevier, 2007, p. 172-173.

⁹ SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25. ed. São Paulo: Malheiros, 2006, p. 241.

¹⁰ Idem. *Ibidem*, p. 243.

indispensável nas relações humanas, funcionando enquanto ferramenta de comunicação, trabalho e lazer. Neste contexto, quebrou-se totalmente o conceito de que seria possível um exercício irrestrito da liberdade na rede, em que pese ser pacífico que a *Internet* redimensionou os limites da liberdade.

Os direitos quanto à liberdade na *Internet* estão intimamente ligados aos direitos de liberdade de comunicação e informação, previsto na Constituição Federal de 1988. Neste sentido, entende, quanto à liberdade informática, Paesani¹¹:

A liberdade informática é o direito de dispor da informação, de preservar a própria identidade informática, isto é, de consentir, controlar, retificar os dados informativos relativos à própria personalidade. Ao direito de informar e ser informado uniu-se o direito de tutelar a "liberdade de informação" como bem pessoal e interesse civil.

Nesta linha, o exercício abusivo da liberdade de expressão, por exemplo, com o comércio de bens e serviços por meio da rede, muitas vezes, chega a beirar a irracionalidade.

Usando o abalo na credibilidade da rede e nos sistemas de comércio eletrônico, há quem defenda a opinião de que a *Internet* precisa de maior controle e regulamentação. Alguns sites de hackers chegam a dizer que os verdadeiros responsáveis pela ação são governos e setores conservadores, que buscam um motivo para limitar a liberdade dos usuários na rede. Para os que sustentam tal posição e que defendem insistentemente a chamada liberdade virtual, o direito específico e regulador das questões da criminalidade na rede será sempre encarado como uma "camisa de força" imposta pelos poderes estatais; afinal, segundo os mesmos, o ciberespaço deveria ser regido com base em um sistema que ultrapassa o liberalismo *lato sensu* e beira o anarquismo, onde toda a forma de interferência dos poderes constituídos revelar-se-ia no mínimo inaceitável e, por isso mesmo, ilegítima.¹²

Entende-se que uma das características mais marcantes do ciberespaço é o dinâmico acesso à informação e a constante propagação de idéias, pensamentos e opiniões, que ocorrem livremente, partindo de todos usuários, de forma simultânea à vontade do emissor. Paesani¹³ destaca a velocidade ímpar da *Web*.

¹¹PAESANI, Lílana Minardi. **Direito de Informática: Comercialização e Desenvolvimento Internacional do Software**. 3. ed. São Paulo: Atlas, 2001, p. 33.

¹²DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Cybercrimes. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & Internet**. Aspectos Jurídicos Relevantes. Bauru: Edipro, 2000, p. 118.

¹³PAESANI, Lílana Minardi. **Direito e Internet...** Op. Cit., p. 18.

Por sua vez, explica Lévy¹⁴ que as telecomunicações geram um dilúvio de informações porque possuem uma natureza exponencial, explosiva e caótica, de modo que cada vez mais aumentam os dados disponíveis, a densidade dos *links* e os contatos entre os indivíduos.

Outra característica relevante no tocante à liberdade na Internet, se dá pelo anonimato do usuário na rede. Muitas vezes os usuários aproveitam deste sigilo propiciado pela rede para utilizar de sua liberdade além dos limites que é permitido, ora que acreditam não haver punição para as suas condutas, se agirem de maneira oculta:

O cyber-espço, por prescindir da presença física dos indivíduos, cria um anonimato. Alguns autores defendem que este anonimato contribui para estabelecer uma condição mais paritária de participação no debate, já que as desigualdades do mundo real (estigmatizações culturais, de classe e de gênero; papéis sociais, diferenças de *status*; habilidade retórica dos participantes, etc.) sofrem um certo apagamento [...]. Se a discussão acontece em um ambiente livre de medo, de intimidação ou de ridículo, uma variedade maior de pontos de vista pode ser expressa.¹⁵

O ocultismo proporcionado aos usuários cria a ilusão de um ambiente livre para a prática de todos os atos. Verifica-se que o usuário cria a expectativa de poder utilizar a ferramenta virtual da forma que melhor lhe convém, sem raciocinar sobre as consequências que seus atos podem causar.

É neste quadro peculiar de dinamismo que se desenvolve o exercício da liberdade na *Internet*, o qual não prejudica, por sua vez, os modos de caracterização de atos ilícitos. As condutas praticadas no ambiente virtual, tanto quanto as cometidas fora dele, são plenamente tangíveis e, caso produzam danos, acarretarão punição. Em linhas gerais, a liberdade no ambiente virtual é agregada por limites que visam à organização e regulamentação deste espaço, buscando coibir ou punir a prática de atos criminosos, ou que possam causar qualquer tipo de dano aos direitos difusos,

¹⁴LÉVY, Pierre. **Cibercultura**. Tradução Carlos Irineu da Costa. 2. ed. São Paulo: Editora 34, 2003, p. 13.

¹⁵ MAIA, Rousiley C. M. **Democracia e a Internet como esfera pública virtual: aproximando as condições do discurso e da deliberação**. Disponível em: <<http://vsites.unb.br/fac/comunicacaoepolitica/Rousiley2001.pdf>>. Acesso em: 09 jun. 2012.

coletivos, individuais homogêneos e puramente individuais, assegurando a segurança jurídica e a paz social. Não existe, em nenhum campo social, seja na *Internet*, seja na vida em sociedade como um todo, o exercício irrestrito da liberdade. Em decorrência de tais limitações, naturalmente surgirão conflitos em casos de abuso do direito de liberdade.

3 Conflitos no ciberespaço e a consequente prática de atos ilícitos

Atualmente tem-se observado os crescentes conflitos criados no ciberespaço. O termo ciberespaço é de uso corrente, apontando a relação humana com a máquina, que no caso é o computador, *tablet*, celular ou qualquer outro instrumento capaz de conectar a *Internet*. Trata-se de um termo que visa explicar a associação de máquinas com as diversas redes, de modos distintos.

Quanto ao cerne destes conflitos, destaca-se que com o surgimento da *Internet*, adveio a ideia de que as atitudes que nela ocorressem não teriam implicação prática, considerada a virtualidade do ciberespaço, numa defesa que ultrapassava o liberalismo.¹⁶ Contudo, uma corrente mais racional despontou porque "toda liberdade, por mais ampla que seja, encontra limites, que servem para garantir o desenvolvimento ordenado da sociedade e dos direitos fundamentais de qualquer sujeito [...]"¹⁷.

O abuso do direito de liberdade vai de encontro, na maior parte das vezes, com os direitos de privacidade e de personalidade, principalmente devido às diversas possibilidades de manifestação do pensamento. O primeiro é composto, conforme Motta e Barchet¹⁸, pela intimidade, que envolve a esfera mais secreta de cada um, e pela vida privada, referente à externalização desta esfera secreta num espaço privado. Já o segundo envolve a proteção da

¹⁶ DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Op. Cit., p. 118.

¹⁷ PAESANI, Líliliana Minardi. **Direito e *Internet***... Op. Cit., p. 24.

¹⁸ MOTTA, Sylvio; BARCHET, Gustavo. Op. Cit., p. 180.

honra e da imagem, isto é, das qualidades da pessoa e de seu aspecto físico, respectivamente¹⁹. No entender de Paesani²⁰, "[...] é evidente que o direito à privacidade constitui um limite natural ao direito à informação".

Outro conflito que pode ser vislumbrado é o da violação aos direitos de propriedade intelectual na defesa de uma liberdade de informação irrestrita. É incontestável que o conceito de propriedade intelectual sofreu mutações e o fator determinante para tanto foi a tecnologia. Sob o enfoque do direito à liberdade, é livre a divulgação de toda informação e o acesso aos dados disponíveis na rede, independente da fonte ou da autoria. Por outro lado, na *Internet* subsistem os mesmos direitos autorais do que no plano concreto, sendo esta a posição de Gandelman²¹ e Paesani²². Segundo Peck²³, nem todo conteúdo da *Internet* é de domínio público.

Assim, as relações do indivíduo com a máquina, ou seja, a ligação entre diversas máquinas comandada por distintas pessoas pode gerar divergências que dão origem a conflitos, que devem ser objeto de intervenção pelo Direito, preservando a pacificação social. Destes conflitos se originam os atos ilícitos em geral, entre os quais se destacam os chamados cibercrimes.

Segundo entendimento de Guimarães e Furlaneto Neto²⁴ (2003, p. 69), cibercrime significa "qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados".

O direito de punir do Estado está ligado a diretrizes normativas que devem ser respeitadas, antes de se considerar uma conduta

¹⁹ SILVA, José Afonso da. Op. Cit., p. 209.

²⁰ PAESANI, Lílana Minardi. **Direito e Internet...** Op. Cit., p. 49.

²¹ GANDELMAN, Henrique. **De Gutenberg à Internet**. Direitos Autorais das Origens à Era Digital. 5. ed. São Paulo: Record, 2007, p. 59.

²² PAESANI, Lílana Minardi. **Direito e Internet...** Op. Cit., p. 67.

²³ PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002, p. 57.

²⁴ GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na *Internet*: elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, Brasília, v. 7, n. 20, jan./mar. 2003, p. 69.

como criminosa. O artigo 5º da Constituição Federal, no inciso XXXIX, prevê que "não haverá crime sem lei anterior que o defina, nem pena sem prévia cominação legal"²⁵. No mesmo sentido, o teor do artigo 1º do Código Penal Brasileiro²⁶.

Neste sentido, Santos²⁷ entende que "deve a lei penal, desta forma, exclusivamente, editar limitações casuísticas, fora das quais tudo é permitido, ou seja, é lícita qualquer conduta que não se enquadre nas normas penais incriminadoras". Reforçam o posicionamento de Lima e Daoun²⁸ quando observam que "não pode ser considerado crime, conduta que não esteja prevista em lei, bem como a que foi formulada sem a observância do devido processo legislativo. É a prevalência dos princípios da reserva legal e da legalidade".

A partir daí, tecem-se 2 aspectos centrais: o primeiro é o de que o uso do computador enquanto meio para a prática de um crime não o descaracteriza; o segundo é o de que não há demérito algum numa conduta danosa não ser considerada crime, pois isso não impede a aplicação de sanções em outras esferas.

Em geral, os cibercrimes podem ser praticados por pessoas que possuem ou não conhecimento especial sobre a rede. Aqueles agentes que possuem um conhecimento diferenciado e particular da rede, especialmente quanto à tecnologia informática, por exemplo, referente a conteúdos e programas que fazem este ambiente funcionar, são denominados como *hackers*. Entretanto,

²⁵ BRASIL. **Constituição da República Federativa do Brasil de 5 de outubro de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 10 fev. 2012.

²⁶ Idem. **Decreto-lei n. 2848 de 07 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 10 fev. 2012.

²⁷ SANTOS, José Eduardo Lourenço dos. **Proteção da Privacidade na Internet: Aspectos Criminais**. 2002. 129f. Dissertação (Mestrado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino “Eurípides Soares da Rocha”, Marília, 2002, p. 63.

²⁸ LIMA, Gisele Truzzi de; DAOUN, Alexandre Jean. **Crimes Informáticos: o Direito Penal na Era da Informação**. Disponível em: <<http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf>>. Acesso em: 03 nov. 2009.

por conta da massificação das ferramentas virtuais, da constante evolução da informática e das facilidades que este processo tem possibilitado aos usuários, uma pessoa sem grandes conhecimentos técnicos pode praticar normalmente um cibercrime; é o caso, *v.g.*, daquela pessoa que se utiliza dos populares sites de relacionamentos para caluniar, difamar ou injuriar outra.

Percebe-se que um *hacker* que invade uma conta bancária e de lá retira valores, transferindo-os para sua conta pessoal, pratica crime de furto; aquele que propositalmente divulga vírus para um inimigo pessoal, gerando destruição do computador, pratica crime de dano; uma pessoa que propaga mensagens ofensivas a outrem, acusando-a de determinado fato ou crime, ou mesmo denegrindo sua imagem genericamente, pratica algum crime contra a honra.

Não importa se foi utilizada a *Internet*, mas sim se configuraram-se os elementos do tipo penal, caso em que haverá crime, independente da prática do ato ter se desenvolvido por completo no ambiente virtual. Com efeito, quebra-se qualquer alegação de que as práticas de atos criminosos no ciberespaço está avessa à aplicação do direito penal, bastando para tanto a configuração dos elementos do crime, não importando o meio de execução.

Pelo que se depreende do exposto neste tópico, percebe-se que se ausentes os elementos do crime, um fato que cause dano não será considerado um ilícito penal. De fato, há práticas usuais na *Internet*, que causam dano ou perturbação da tranquilidade social, que não se encontram tipificadas criminalmente. Como se verá no tópico a seguir, há iniciativas legislativas no sentido de modificar esta situação, notadamente devido à crença consolidada no Legislativo de que só o direito penal é um remédio para a realização da justiça.

No entanto, o direito penal enquanto *ultima ratio* tem sido a diretriz seguida majoritariamente hoje. Assim, caberá a tutela penal apenas quando os bens jurídicos atingidos forem tão relevantes a ponto de a tutela por outro ramo do Direito ser ineficaz, ou seja, não conferir a resposta social esperada.

Em termos de danos causados na *Internet*, a principal tutela alternativa se dá pelo instituto da responsabilidade civil, adotando-

se o conceito do artigo 186 do Código Civil: "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito"²⁹. Em complemento, prevê o artigo 927: "aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo"³⁰. No instituto da responsabilidade civil, existem as modalidades contratual, quando o ato danoso ocorreu em razão de uma obrigação pré-existente, contrato ou negócio jurídico unilateral; e extracontratual, se resultante de um dever de conduta violado, de uma transgressão de comportamento, sem que exista negócio jurídico prévio³¹. Em se tratando de ilícitos cometidos na rede, existirão casos contratuais, por exemplo, nas relações de consumo e demais contratos firmados, bem como, e principalmente, ilícitos extracontratuais, decorrentes de todas as atitudes danosas praticadas pela *Web* (neste ponto entra a fórmula genérica de tutela judicial, independentemente da ausência de previsão específica a título criminal, garantindo-se a reparação do dano e a compensação do agente por outra via). Sobre a responsabilidade civil na *Internet*, explica Gonçalves³²:

A responsabilidade extracontratual pode derivar de inúmeros atos ilícitos, sendo de se destacar os que dizem respeito à concorrência desleal, à violação da propriedade intelectual, ao indevido desrespeito à intimidade, ao envio de mensagens não desejadas e ofensivas da honra, à divulgação de boatos infamantes, à invasão de caixa postal, ao envio de vírus etc. Identificado o autor, responde ele civilmente pelos prejuízos causados a terceiros.

Prenchidos os requisitos legais, haverá dever de indenizar, o que demonstra que o dano causado não ficará impunível. Deveras, não somente a tutela penal é instrumento de compensação/punição pelo dano causado por meio da *Internet*, funcionando principalmente a tutela cível, pela responsabilidade civil

²⁹ BRASIL. **Lei n. 10406 de 10 de janeiro de 2002**. Código Civil. Disponível em: <<http://www.planalto.gov.br/ccivil/leis/2002/L10406.htm>>. Acesso em: 10 fev. 2012.

³⁰ Idem. *Ibidem*.

³¹ VENOSA, Sílvio de Salvo. **Direito Civil: Responsabilidade Civil**. 6. ed. São Paulo: Atlas, 2006. v. 4, p. 18-19.

³² GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 9. ed. São Paulo: Saraiva, 2005, p. 119.

extracontratual, como regra genérica que autoriza a punição numa infinidade de casos.

Com efeito, não há porque a postura legislativa buscar tipificar taxativamente os atos ilícitos possíveis na *Internet* enquanto crimes, o que somente engessaria a rede, pois a tutela cível atende bem às exigências punitivas da *Web* quando não há tipo criminal específico, garantindo a reparação financeira do dano.

4 Postura estatal a respeito do exercício da liberdade na *Web*

Como visto até agora, dois pressupostos devem ser considerados para se estudar a postura estatal quanto ao exercício da liberdade na rede mundial de computadores: o primeiro é o de que, seguindo um conceito jusfilosófico, o direito à liberdade não pode ser exercido de forma abusiva; o segundo é o de que, havendo abuso, será configurado um ato ilícito, aplicando-se a lei penal quando houver tipo legal correspondente, sem prejuízo do uso do instituto da responsabilidade civil (cumulada ou subsidiariamente).

No Brasil e no mundo a *Internet* se consolidou como um instrumento fundamental para criar e manter as relações humanas. É inegável a influência desta ferramenta em diversas áreas e grupos sociais, da esfera empresarial à particular, do âmbito público ao privado. Os três Poderes, quais sejam o Legislativo, Executivo ou Judiciário, têm utilizado cada vez mais a rede como forma de aproximar a sociedade dos atos por eles praticados, bem como de tornar mais eficiente a prestação de serviços públicos.

Merece destaque o Poder Judiciário, que cada dia mais agrega a *Internet* aos atos processuais. As intimações eletrônicas e o envio de petição pela rede são exemplos da forma como a Justiça tem utilizado a tecnologia, visando à celeridade processual.

Por outro lado, a mesma *Internet* que geralmente é utilizada para fins pacíficos tem causado grandes transtornos no mundo fático-jurídico, demandando uma intervenção cada vez maior do Estado

para solucionar conflitos oriundos deste meio, tanto na esfera cível quanto na penal.

Estatísticas apontam que no ano de 2002 havia no judiciário brasileiro cerca de 400 decisões envolvendo problemas virtuais. Já em 2008, esse número ultrapassava 17 mil ações, tendendo cada vez mais este número se elevar.³³

Recentemente, o governo brasileiro foi assolado por uma série de ataques à segurança nacional, onde sites como o da Presidência da República, do Portal Brasil, da Receita Federal e da Petrobras foram invadidos e retirados do ar, atribuindo-se a autoria a hackers italianos. A gravidade deste ataque foi tamanha que até mesmo dados pessoais de políticos foram expostos, por exemplo, o Cadastro de Pessoa Física (CPF) da atual Presidente da República, Dilma Rousseff, demonstrando a vulnerabilidade sistêmica a ataques eletrônicos.³⁴

Também ilícitos entre particulares têm ocorrido com frequência, ensejando principalmente condenações cíveis que visam reparar os danos causados, sem prejuízo às devidas condenações criminais, quando for o caso. Neste sentido, tem entendido o Tribunal de Justiça do Estado de São Paulo que a prática de ilícitos cometidos no ambiente virtual gera dever de indenizar:

DANO MORAL - TEXTO INSERIDO EM COMUNIDADE DE SITE DE RELACIONAMENTO NA *INTERNET* (ORKUT) - DIZERES OFENSIVOS, COM TERMOS CHULOS, CAPAZES DE PRODUZIR SÉRIA OFENSA MORAL - MAGNITUDE DO ALCANCE DA OPINIÃO INSERIDA NA REDE MUNDIAL, EM SITE DESTINADO AO RELACIONAMENTO DE PESSOAS, SOBRE FIGURA PÚBLICA, EM CIDADE DO INTERIOR -

³³DINIZ, Laura. Justiça Derruba Anonimato e Pune Cada Vez Mais por Crimes na *Internet*. **O Estado de São Paulo**. São Paulo, p. C1, 01 out. 2008.

³⁴SILVEIRA, Igor; RIZZO, Alana; PARIZ, Tiago. Até dados pessoais de Dilma Rousseff são divulgados por hackers. **Correio Braziliense on-line**, 24 junho 2011. Disponível em: <http://www.correiobraziliense.com.br/app/noticia/politica/2011/06/24/interna_politica,258240/ate-dados-pessoais-de-dilma-rousseff-sao-divulgados-por-hackers.shtml>. Acesso em: 12 maio 2012.

DANO MORAL CARACTERIZADO - INDENIZAÇÃO FIXADA - APELAÇÃO DESPROVIDA.³⁵

O caso acima relata a ofensa ao direito de personalidade da vítima, na faceta da honra, o que é apto a gerar punição criminal pela prática de crime contra a honra, bem como dever de indenizar moral e materialmente na esfera cível. Não são poucos os casos semelhantes, abrangendo a prática de crimes contra a honra em suas três modalidades (calúnia, injúria e difamação), até mesmo porque não se exige do agente que comete o ilícito qualquer conhecimento técnico especial. Afinal, com as redes sociais tornou-se fácil criar um perfil no qual podem ser divulgadas informações variadas, inclusive dotadas de conteúdo ilícito.

Segundo Pinheiro³⁶, os crimes contra a honra são os casos mais comuns entre os usuários de qualquer idade e muitas vezes o infrator age com negligência ou ingenuidade, pois acredita que não está prejudicando alguém, mas apenas manifestando sua opinião ao falar mal de professores, colegas, artistas e políticos.

Não obstante, o particular pode ser vítima de um hacker, que utiliza-se de conhecimento técnico privilegiado e da ingenuidade do internauta para acessar informações privilegiadas, como senhas bancárias e dados cadastrais. Com isso, comete crimes como furto e estelionato, também havendo o dever de indenizar.

Nesta linha, os cavalos de troia, além de servirem para destruir dados eletrônicos alheios, podem deixar o sistema vulnerável sob o aspecto de proteção de dados. Esse código malicioso poderá instalar programas que possibilitem o controle do invasor sobre o computador, permitindo o acesso a arquivos nele armazenados, bem como a senhas bancárias, além de possibilitar a formatação do disco rígido³⁷. Não obstante, é possível o roubo de informações e

³⁵ SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação n. 9110832-40.2006.8.26.0000**. Relator: Elliot Akel. São Paulo, 20 de outubro de 2010. Disponível em: www.tj.sp.gov.br. Acesso em: 15 nov. 2011.

³⁶ PINHEIRO, Patrícia Peck. **Uso Ético e Responsável da Internet**. Dicas e Alertas. São Paulo: Fundação Bradesco, 2009, p. 09.

³⁷ BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para a Internet**, parte VIII: Códigos Maliciosos

dados pessoais, como números de cartões de créditos, senhas e dados de contas, por meio de sites e e-mails fraudulentos, o que é chamado de *phishing*³⁸. Ao contrário do cavalo de troia, o *phishing* não se instala no computador, ou seja, não constitui um *software*, sendo enviado aos usuários com mensagens visando enganá-los para fornecerem determinados dados.

Todas as informações apontadas desde o início deste tópico demonstram que o contexto da prática de atos ilícitos sofreu relevante alteração com o advento da *Internet*, implicando na necessidade de uma nova postura do Poder Judiciário. Por vezes, tal postura requer a adoção de um posicionamento minimalista, priorizando a reparação cível do dano em detrimento da penal, notadamente quando não houver mera variação de meio para a configuração do fato típico. De outro lado, crimes previstos no ordenamento jurídico pátrio ganharam novas formas, geralmente mais graves, diante da maior repercussão do ilícito pelo efeito potencializador da *Web*. Naturalmente, passou-se a discutir qual solução o ordenamento jurídico deveria dar para a questão, ou seja, qual postura deveria ser tomada pelo Legislativo brasileiro. O Judiciário tem se utilizado de técnicas de Nova Hermenêutica Constitucional para os casos em que não há disciplina jurídica específica, o que tem surtido bons efeitos, garantindo a punição dos ilícitos sem prejudicar o dinamismo da rede. O Legislativo deve ficar atento a este contexto, não regulamentando sem necessidade a rede, o que a faria perder seu caráter democrático.

Não se pode perder de vista que a tendência do Poder Legislativo brasileiro é a de legislar intensamente sobre assuntos que chamem a atenção da sociedade, geralmente por motivos políticos e não técnicos. Costuma-se criticar este excesso legislativo, pois os legisladores se perdem em normas confeccionadas sem qualidade técnica ou utilidade prática, fadadas à ineficácia.

(*Malware*). Disponível em: <<http://cartilha.cert.br/download/cartilha-08-malware.pdf>>. Acesso em: 04 out. 2010.

³⁸MICROSOFT. **Phishing**: Perguntas Frequentes. Disponível em: <<http://www.microsoft.com/brasil/protect/yourself/phishing/faq.msp>>. Acesso em: 05 out. 2010.

Em 2011, aliás, foi aprovado um total de 207 leis federais, correspondentes da Lei n. 12.379, de 06 de janeiro de 2011, até a Lei n. 12.586, de 30 de dezembro de 2011; além das Leis Complementares n. 139 e 140, respectivamente em 10 de novembro e 8 de dezembro do corrente ano; e da Emenda Constitucional n. 68, de 21 de dezembro de 2011³⁹. Assim, o total foram de 210 novos diplomas legais incorporados ao ordenamento jurídico brasileiro no âmbito federal, excluídos decretos e decretos-legislativos, lembrando que os últimos são os responsáveis por levar a conhecimento público os tratados internacionais que deverão ser cumpridos interna e externamente pelo Brasil. O simples fato de uma Constituição Federal com 23 anos já ter recebido 70 emendas (EC n. 70, de 29 de março de 2012) evidencia a forte tendência legislativa brasileira.

No âmbito dos crimes da *Internet*, forte corrente do Poder Legislativo tem pretendido criar um número cada vez maior de tipos penais incriminadores, tantas vezes quanto se mostrar necessário para coibir ilícitos na rede. Neste sentido, o parecer da CCJ no PL n. 84/1999, que será estudado em detalhes a frente:

É exatamente em cima dessas ações que apresentam aspectos específicos que devemos atentar trabalhando para tipificar um número cada vez maior de ações que, devido a mobilização dos dados no sistema de informática, se multiplicam e se diversificam rapidamente, violando direitos e fazendo da *Internet* instrumento para a prática de crimes.⁴⁰

Em geral, verifica-se que esta tendência, no entanto, não abrange questões relevantes ao interesse social, mas servem como instrumento de política, autopromoção e atendimento aos clamores sociais tão comuns quando deflagradas tragédias do cotidiano. Sem uma atenção a tal crítica, tão usual no meio jurídico, qualquer estudo da questão legiferante na *Internet* restará invariavelmente incompleto.

³⁹BRASIL. Congresso Nacional. **Legislação**. Disponível em: <<http://www2.planalto.gov.br/presidencia/legislacao>>. Acesso em: 12 maio 2012.

⁴⁰BRASIL. Poder Legislativo. Câmara dos Deputados. **Parecer da Comissão de Constituição e Justiça no Projeto de Lei n. 84 de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 10 maio. 2012.

Estabelecidos os devidos pressupostos fáticos, no presente, são levantadas duas propostas legislativas em curso no Congresso Nacional, uma adotando posição mais favorável ao aumento de criminalizações, outra priorizando a tutela cível em prol da liberdade do usuário: o Projeto de Lei n. 84/1999, que "dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências"⁴¹, e o recente anteprojeto de Lei encaminhado pela Presidente da República ao Congresso Nacional, PL n. 2126/2011, intitulado como "Marco Civil da Internet"⁴².

4.1 *Projeto de Lei Azeredo: Projeto de Lei n. 84/1999*

Desde 1999, está em trâmite no Poder Legislativo Brasileiro o Projeto de Lei n. 84 (PL n. 84/1999), também conhecido como "Projeto de Lei Azeredo", que "dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências", o qual "caracteriza como crime informático ou virtual os ataques praticados por 'hackers' e 'crackers', em especial as alterações de *home pages* e a utilização indevida de senhas"⁴³.

Embora o projeto seja de autoria do ex-deputado federal Luiz Piauhyllino (PSDB/PE), as mais relevantes alterações no projeto foram de autoria do Senador Eduardo Brandão de Azeredo (PSDB/MG), que apresentou um Projeto de Lei substitutivo (PLC n. 89/2003) e tem adotado postura ativa pela sua aprovação.

Dentre as questões que tal projeto pretende regular, destacam-se: acesso indevido ao meio eletrônico; manipulação ilícita de informação virtual; difusão e propagação de vírus; atentado contra a segurança de serviços de utilidade pública; obtenção,

⁴¹Idem. **Projeto de Lei n. 84 de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 10 maio 2012.

⁴²Idem. _____. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 2.126 de 24 de agosto de 2011**. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>>. Acesso em: 10 maio 2012.

⁴³Idem. **Projeto de Lei n. 84...** Op. Cit.

transferência ou fornecimento não autorizado de dados eletrônicos; divulgação ou utilização indevida de informações e dados pessoais; estelionato na rede; falsificação de dados eletrônicos; entre outros⁴⁴.

Verifica-se que o Projeto de Lei n. 84/1999, aprovado pelo Senado Federal, além de ter obtido dois pareceres de comissões totalmente favoráveis à aprovação na Câmara dos Deputados (entre elas a Comissão de Constituição e Justiça), está repleto de controvérsias que inviabilizam sua aplicabilidade e eficácia no ordenamento jurídico, em caso de aprovação. Ainda assim, consta no parecer da Comissão de Constituição e Justiça:

Quanto aos aspectos constitucional, jurídico e de boa técnica, a proposta em questão atende aos pressupostos formais e materiais previstos na Constituição federal e está em conformidade com os princípios e normas do ordenamento jurídico brasileiro. [...] A preocupação que surge é que, juntamente com a evolução das técnicas na área da informática, a sua expansão foi acompanhada por aumento e diversificação das ações criminosas, que passaram a incidir em manipulações de informações, difusão de vírus eletrônico, clonagem de senhas bancárias, falsificação de cartão de crédito, divulgação de informações contidas em bancos de dados, dentre outras. [...] ⁴⁵

Percebe-se que a CCJ acabou fazendo uma análise genérica do Projeto de Lei, sem se ater aos seus aspectos técnicos. Aliás, não comentou sequer uma das propostas de alteração da legislação brasileira. O trecho colacionado foi o mais específico encontrado no parecer, que em apenas 3 páginas se limitou a comentar as polêmicas que cercam a questão legiferante na *Internet* e afirmou de forma genérica que o projeto atende à boa técnica.

De tudo o que tem sido dito pelos legisladores a respeito do projeto, depreende-se que ele tem a finalidade de se tornar a primeira lei no ordenamento jurídico brasileiro que regule de forma ampla e objetiva os crimes cibernéticos. Entretanto, há grupos de estudiosos, doutrinadores e usuários da *Internet*, que entendem que, se aprovado, o projeto causará grande ameaça ao direito à privacidade dos cidadãos, além de um atentado ao direito de liberdade, prejudicando a democracia digital.

⁴⁴ Idem. *Ibidem*.

⁴⁵ Idem. **Parecer da...** Op. Cit.

Se não bastasse, este mesmo projeto sofre grande resistência por parte dos usuários da *Internet*, tendo em vista que circula na rede uma petição eletrônica, com mais de 165 mil assinaturas, de pessoas que se opõem à aprovação, alegando ser uma afronta à democracia e à liberdade na *Web*. Consta no teor da petição intitulada "Em defesa da liberdade e do progresso do conhecimento na *Internet* brasileira":

[...] Um projeto de Lei do Senado brasileiro quer bloquear as práticas criativas e atacar a *Internet*, enrijecendo todas as convenções do direito autoral. O Substitutivo do Senador Eduardo Azeredo quer bloquear o uso de redes P2P, quer liquidar com o avanço das redes de conexão abertas (*Wi-Fi*) e quer exigir que todos os provedores de acesso à *Internet* se tornem delatores de seus usuários, colocando cada um como provável criminoso. É o reino da suspeita, do medo e da quebra da neutralidade da rede. Caso o projeto Substitutivo do Senador Azeredo seja aprovado, milhares de internautas serão transformados, de um dia para outro, em criminosos. Dezenas de atividades criativas serão consideradas criminosas pelo artigo 285-B do projeto em questão. Esse projeto é uma séria ameaça à diversidade da rede, às possibilidades recombinantes, além de instaurar o medo e a vigilância.⁴⁶

Referida petição demonstra a preocupação dos próprios internautas de que o Poder Legislativo adote uma diretriz policialesca com relação à rede mundial de computadores, tornando o acesso mais difícil, limitado e oneroso.

A preocupação é compreensível e relevante. Afinal, a principal marca da rede é o seu caráter democrático e libertário, permitindo ao usuário transpor fronteiras culturais, pessoais e territoriais. O principal benefício que a *Internet* trouxe foi a capacidade ampla de informar e ser informado.

"Pode-se afirmar que o grau de democracia de um sistema pode ser medido pela quantidade e qualidade de informação transmitida e pelo número de sujeitos que a ela tem acesso"⁴⁷. Nesta seara, "quanto maior a diversidade de mensagens e de participantes, mais alta será a massa crítica da rede"⁴⁸. Uma limitação excessiva da

⁴⁶ COMUNIDADE DE CIBERCULTURA. **Pelo veto ao projeto de cibercrimes:** Em defesa da liberdade e do progresso do conhecimento na *Internet* Brasileira. Disponível em: <<http://www.petitiononline.com/veto2008/petition.html>>. Acesso em: 12 maio 2012.

⁴⁷ PAESANI, Lílana Minardi. **Direito e *Internet*...** Op. Cit., p. 23.

⁴⁸ CASTELLS, Manuel. **A Sociedade em Rede**. 9. ed. São Paulo: Paz e Terra, 2006. v. 1, p. 439.

liberdade de informação na *Internet*, invariavelmente, gerará uma diminuição de seu caráter democrático.

Entre outras alterações, caso vire lei, o PL citado irá alterar os artigos 265 e 266 do Código Penal Brasileiro, passando a ser crime atentar contra, interromper ou perturbar serviços de informação ou telecomunicação. Desta forma, observa-se a previsão de um novo capítulo no respectivo código, intitulado "Dos Crimes contra a Segurança dos Sistemas Informatizados", a ser acrescido no Título VIII, "Dos Crimes contra a Incolumidade Pública".⁴⁹

Na atualidade, a maior forma de se atentar contra o sistema virtual, é através da propagação e difusão de códigos maliciosos, os chamados vírus. A conduta seria uma espécie de crime contra a incolumidade pública, reforçando a coerência de se inserir em tal título da legislação, conforme supracitado, protegendo assim, os interesses difusos. No entanto, não serão estas as condutas abrangidas pelo novo capítulo, mas sim as de acesso mediante violação de segurança (artigo 285-A, CP) e de obtenção ilegítima de dado ou informação (artigo 285-B, CP)⁵⁰. Tratam-se de condutas que geralmente atingirão uma pessoa específica, salvo se a informação acessada ou a violação de segurança sejam praticados contra a Administração (ainda assim, poderia se enquadrar melhor como crime contra a Administração). Neste viés, até faz sentido a exigência de representação (artigo 285-C, CP - exigência de representação, salvo se a vítima for, de algum modo, o serviço público - p. ex., União, fundações públicas, serviços sociais autônomos⁵¹), mas esta é inaceitável se os crimes em questão forem realmente considerados como crimes contra a incolumidade pública. A figura da representação é incompatível com a natureza do crime contra a sociedade, ou a incolumidade pública, posto que a vítima nestes crimes será protegida de forma reflexa, bem como possíveis danos a ela causados. Afinal, nos crimes que visam proteger a incolumidade, são vislumbradas condutas que podem

⁴⁹ BRASIL. Projeto de Lei n. 84... Op. Cit.

⁵⁰ BRASIL. Projeto de Lei n. 84... Op. Cit.

⁵¹ Idem. Ibidem.

perturbar a tranquilidade dos indivíduos, lesando bens ou interesses indispensáveis à sobrevivência do homem; são protegidos interesses difusos, sem titulares identificáveis⁵².

A conduta que mais se aproxima de um crime contra a incolumidade pública seria o crime de "inserção ou difusão de código malicioso" que, por sua vez, foi considerado um crime de dano (artigo 163-A, CP)⁵³. A divulgação de código malicioso é uma das maiores perturbações na *Internet*, prejudicando o seu bom funcionamento ao deteriorar o seu conteúdo e os computadores a ela conectados. Tais Códigos se propagam pela rede e atingem imensas proporções, sendo geralmente impossível detectar o número de prejudicados. Descobrimo-se a origem de um vírus que se disseminou na rede, nada mais coerente do que processar o agente pela prática de crime contra a incolumidade pública. Esta parece ser uma conduta penalmente relevante a título de tipificação de crimes cibernéticos, porque o dispositivo que melhor se enquadra na prática em questão é o do artigo 265 do Código Penal, que prevê: "atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública: Pena - reclusão, de um a cinco anos, e multa"⁵⁴. No caso, sem dúvidas a *Internet* pode ser considerada um outro serviço de utilidade pública, mas a falta de especificidade do tipo pode gerar uma interpretação restritiva por parte dos magistrados, deixando uma conduta penalmente relevante desprotegida nesta esfera.

Parece ser esta a *ratio legis* da proposta de alteração na redação do referido dispositivo, bem como do que o sucede, incluindo a informação e a telecomunicação, isto é, a questão informática como objetos jurídicos protegidos⁵⁵. Então, se o redator do PL n. 84/1999 propôs novas redações aos artigos 265 e 266, que tratam dos crimes contra a incolumidade pública, inserindo expressamente a proteção da *Internet* como abrangida pelos tipos,

⁵² JESUS, Damásio Evangelista de. **Direito Penal**. 15. ed. São Paulo: Saraiva, 2003. v. 2, p. 267.

⁵³ BRASIL. **Projeto de Lei n. 84...** Op. Cit.

⁵⁴ Idem. **Decreto-lei n. 2848...** Op. Cit.

⁵⁵ Idem. **Projeto de Lei n. 84...** Op. Cit.

qual a necessidade de outro tipo específico sobre a inserção de códigos maliciosos?

Este outro tipo específico, ao que consta, servirá apenas para proteger a divulgação de Código malicioso que tome pequenas proporções, ou seja, volte-se para um computador específico ou para uma empresa específica ou para alguma rede fechada específica. Retirada a nota de especificidade, o crime já seria contra a incolumidade pública. É preciso, ainda, considerar: a) geralmente, quando se divulga um Código malicioso na *Web* se busca atingir o maior número possível de pessoas; b) a simples divulgação de um Código malicioso na rede mundial de computadores, ainda que retido em estágio inicial, já caracterizaria um crime contra a incolumidade pública, que não exige dano concreto.

Ainda que se adote uma postura avessa ao direito penal mínimo, não faz sentido que a tipificação proposta para o artigo 163-A, que por exclusão envolverá a divulgação de Código malicioso em menores proporções para causar danos especificamente a alguém ou a alguma instituição, não exija a efetiva concretização do dano para a consumação. Não parece o que pensa o legislador, que propõe qualificar a nova modalidade de crime de dano caso o dano se verifique (artigo 163-A, §1º)⁵⁶. Caso aprovado o dispositivo, haverá um crime de dano qualificado pelo dano no ordenamento jurídico brasileiro, caracterizando verdadeiro *bis in idem*.

A proposta de redação do artigo 163-A, que cria outra espécie de crime de dano, evidencia outra nota do PL n. 84/99, qual seja o rigor nas propostas de pena privativa de liberdade, evidenciando uma falta de proporcionalidade intensa. Enquanto o Código Penal prevê a pena de 1 mês a 6 meses de detenção ou multa para o dano comum do artigo 163, aumentando-a para 6 meses a 3 anos de detenção e multa na modalidade qualificada do parágrafo único do artigo 163⁵⁷, o PL n. 84/1999 quer que o dano decorrente da divulgação de Código malicioso (que como visto exclui a divulgação desta natureza que caracterize crime contra a

⁵⁶ Idem. *Ibidem*.

⁵⁷ Idem. **Decreto-lei n. 2848...** Op. Cit

incolumidade pública) receba pena de 1 a 3 anos de reclusão e multa caso o dano não se concretize, e de 2 a 4 anos de reclusão e multa caso se verifique⁵⁸.

O Projeto de Lei n. 84/99 (PL n. 84/1999) possui controvérsias que demonstram uma falta de tecnicidade do legislador ao criar normas sobre assuntos em destaque no cenário jurídico. Bem se sabe que a questão de regulamentação da *Internet* é polêmica, sendo preciso encontrar um equilíbrio entre segurança jurídica e preservação do caráter libertário e democrático da rede. Não se justifica a adoção de uma postura policial, mas ainda que assim se faça, é preciso ao menos respeito à melhor técnica jurídica. O apontamento das controvérsias acima deixa claro que, ao contrário do que afirmou o parecer da Comissão de Constituição e Justiça da Câmara, o PL n. 84/1999 está longe de atender à boa técnica.

4.2 O Marco Civil da Internet: Projeto de Lei n. 2126/2011

Em 2011, a presidente da República do Brasil, Dilma Rousseff, encaminhou ao Congresso Nacional o anteprojeto de lei que estabelece princípios, garantias e deveres para o uso da rede mundial de computadores dentro do território nacional. Este anteprojeto no momento se encontra na Câmara dos Deputados, sob o n. 2126/2011, tendo como proposta também a delimitação de deveres e responsabilidades dos prestadores de serviços virtuais, definindo a posição do poder público no tocante ao desenvolvimento social da *Internet*.

O Marco Civil criou um debate frente aos parlamentares em relação o PL n. 84/1999, no qual uns alegam que esta lei com tipos incriminadores é capaz de regular o ciberespaço, e outros entendem que este projeto antigo deve ser retirado de pauta, tendo em vista que estabelece restrições profundas capazes de comprometer o caráter democrático da *Internet*, sendo necessária a aprovação do PL n. 2126/2011. Ademais, há de se destacar que o PL n. 2126/2011 foi criado com base em discussões populares no

⁵⁸ Idem. **Projeto de Lei n. 84...** Op. Cit.

espaço público, tendo sua redação com base na vontade coletiva, diferente do substitutivo proposto pelo Senador Azeredo.

Hoje, esse espaço público não se limita à praça, ao local tradicionalmente aberto ao povo, mas abrange também a *Internet*. A hipótese é que as conexões entre as pessoas estabelecidas pela rede mundial de computadores constituem elas mesmas um fórum de discussões públicas entre iguais, apto a estimular o exercício público de liberdades fundamentais como as de reunião e manifestação.⁵⁹

O exercício da democracia na *Internet* se intensifica quando o cidadão passa a ter o direito de manifestar suas opiniões a respeito dos rumos que deseja ver o país adotar, inclusive no tocante à criação de leis, que atingirão diretamente sua esfera de direitos. Vale lembrar que uma regulamentação da *Internet* [...]

[...] deve estabelecer, portanto, novas fronteiras para a autonomia privada em sua intrincada tarefa de ser instrumento para as liberdades individuais enquanto ressona um conjunto de direitos fundamentais a elas ligados. Para isso, uma forma de regulação é necessária, porém em uma matiz que nem sempre coincide com o dos institutos clássicos do direito civil; a utilização da *soft law* e de cláusulas gerais, aliadas a um trabalho conjunto com outras esferas do ordenamento, podem ser alguns dos caminhos a seguir.⁶⁰

Em geral, parece este o caminho do marco civil da *Internet*, que busca fornecer diretrizes amplas quanto ao tratamento dos conflitos na *Internet*, denotando as prioridades legislativas sempre que necessária a interpretação por parte do jurista. Os primeiros artigos do PL n. 2126/2011 deixam claro o viés que se pretende seguir quanto à aplicação das leis na *Internet*, que é o da democracia, da liberdade e do amplo acesso à informação:

Art. 2º A disciplina do uso da Internet no Brasil tem como fundamentos:

- I - o reconhecimento da escala mundial da rede;
- II - os direitos humanos e o exercício da cidadania em meios digitais;
- III - a pluralidade e a diversidade;
- IV - a abertura e a colaboração; e
- V - a livre iniciativa, a livre concorrência e a defesa do consumidor.

Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

⁵⁹ANDRADE NETO, João; SIQUEIRA, Gustavo Silveira. A revolução será tuitada: como a *Internet* pode estimular o exercício público das liberdades. In: XX Congresso Nacional do CONPEDI, 2011, Vitória/ ES. **Anais do XX Congresso Nacional do CONPEDI**. Florianópolis: Fundação Boiteux, 2011, p. 3443.

⁶⁰VAZ, Ana Carolina. Neutralidade da Rede, Proteção de Dados Pessoais e Marco Regulatório da *Internet* no Brasil. **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, n. 5, jul./dez. 2011, p. 154.

- I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição;
- II - proteção da privacidade;
- III - proteção aos dados pessoais, na forma da lei;
- IV - preservação e garantia da neutralidade da rede, conforme regulamentação;
- V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
- VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
- e
- VII - preservação da natureza participativa da rede.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria, ou nos tratados internacionais em que a República Federativa do Brasil seja parte.⁶¹

Com tais diretrizes, resta claro que não há princípio que prevaleça quando estiver em roga um conflito de interesses no ciberespaço. Ou seja, a segurança jurídica é tão importante quanto a privacidade, a liberdade e o acesso à informação. Neste ponto o PL n. 2126/2011 merece elogios, consubstanciando a vontade dos internautas no sentido de que a rede seja preservada em sua essência, independentemente do interesse de uns e outros. Às vezes, vale a pena abrir mão da proteção de um interesse para que outro, maior, seja garantido da forma mais plena possível. De nada adianta obter plena proteção à privacidade e total garantia à segurança jurídica se com isso não for possível utilizar a *Internet* em seus caracteres centrais, como dinamismo, intensidade de fluxos e prevalência do acesso gratuito.

Esta política é muito diferente da buscada no PL n. 84/1999, que prioriza de forma inequívoca a segurança jurídica, ainda que se perca muito em liberdade do usuário. Uma postura nestes moldes não pode ser aceita, podendo prejudicar a própria essência da *Internet*, o que contraria a vontade social. O equilíbrio de interesses é algo essencial em qualquer sistema jurídico democrático, efetuando-se a ponderação de princípios, com respeito à razoabilidade e à proporcionalidade.

⁶¹ BRASIL. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 2.126 de 24 de agosto de 2011.** Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>>. Acesso em: 10 maio 2012.

Sobre a restrição da liberdade na rede, pondera Cella:⁶²

Qualquer restrição que vier a ser aplicada a essa forma de liberdade quase que ilimitada deve ser muito bem ponderada. Sabe-se que os Estados, mediante o controle social, restringem parcelas de liberdade dos indivíduos e, ainda, que há uma tendência muito forte, por parte do poder, de ampliar tanto quanto possível o seu controle.

Prova do tratamento dispare que pretende ser conferido pelo PL n. 84/1999 em relação ao do PL n. 2126/2011 se refere à tormentosa questão do tratamento de dados:

Enquanto o PL n. 2126/2011 prevê o armazenamento de dados pelos mantenedores de sites da *Internet* pelo prazo de 1 ano, mantendo os registro de conexão (artigo 11)⁶³; o PL n. 84/1999 exige tal armazenamento pelo prazo de 3 anos, com registro da conexão em detalhes, submetendo-se o sistema implementado pelo respectivo site da rede a uma auditoria, sujeitando-se a multa por qualquer requisição de informação não atendida (artigo 22)⁶⁴. Em vez de sustentar um sistema oneroso de armazenamento, sujeito a constante fiscalização por auditorias, o PL n. 2126/2011 limita as informações a serem guardadas pelo provedor (artigos 12 e 13).⁶⁵

As limitações quanto ao tipo de informações que devem ser armazenadas torna menos onerosa a manutenção de bancos de dados registrares, o que favorece a manutenção do caráter predominantemente gratuito do acesso às páginas da *Internet*. Talvez o PL n. 2126/2011 peque ao excluir a responsabilidade do provedor pelo dado que opte por não armazenar (artigo 13, §1º), pois tal faculdade deveria gerar um ônus, qual seja o de indenizar por ato ilícito que o provedor não impediu que ocorresse e nem indicou o responsável pela prática. Parece que tal diretriz contraria a tendência de conferir uma responsabilidade subsidiária às mantenedoras de sites no tocante aos atos ilícitos praticados em seu sítio. É insuficiente para a plena reparação do ato ilícito que se

⁶² CELLA, José Renato Gaziero. Reflexões filosóficas preliminares para o governo eletrônico e democracia digital. **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, n. 1, jul./dez. 2009, p. 53.

⁶³ BRASIL. **Projeto de Lei n. 2126...** Op. Cit.

⁶⁴ Idem. **Projeto de Lei n. 84...** Op. Cit.

⁶⁵ Idem. **Projeto de Lei n. 2126...** Op. Cit.

responsabilize o site apenas pela informação que após requerimento não foi retirada da rede (artigo 15)⁶⁶, pois, ao exercer a faculdade de não armazenar certos dados de acesso pelo prazo de 1 ano, o provedor adquiriu o ônus de reparar danos causados devido ao exercício da faculdade.

Sobre as questões problemáticas a respeito do Marco Civil da *Internet*, sintetiza Vaz⁶⁷:

São três as principais polêmicas do projeto: anonimato na rede, remoção de conteúdo e registro de internautas. O conceito “neutralidade da rede” significa que todas as informações devem ser tratadas da mesma forma e navegar na mesma velocidade. O Marco Civil tenta garantir a neutralidade para todos os internautas brasileiros, num momento em que a discussão sobre o tema atinge o ápice nos EUA - em a autoridade do FCC (Comissão Federal de Comunicações, na sigla em inglês) está sendo questionada. Regular sem censurar, registrar usuários sem invadir a privacidade alheia, proibir o anonimato sem tolher a liberdade de expressão, esses os desafios da regulamentação que se pretende fazer.

Ainda que tais desafios se revelem evidentes e que mesmo o PL n. 2126/2011 tenha os seus pontos que merecem reavaliação por parte do legislador, de maneira genérica, é a proposta que visa preservar de forma mais eficaz o caráter democrático e libertário da *Internet*, atendendo aos interesses dos usuários.

Uma efetiva democracia digital é o principal objetivo a ser alcançado com o debate a respeito da atividade legislativa que tenha por objeto os conflitos da *Internet*. Uma postura ativa dos usuários no processo de discussão a respeito da atuação legislativa tende a beneficiar a efetivação de tal democracia. Com efeito, é o que se depreende de um estudo comparativo do PL n. 84/1999, elaborado sem qualquer participação popular, quanto ao PL n. 2126/2011, discutido na rede antes do envio ao Legislativo.

5 Conclusão

A *Internet* é um instrumento fundamental ao avanço tecnológico na sociedade contemporânea, um espaço para o exercício da liberdade

⁶⁶ Idem. Ibidem.

⁶⁷ VAZ, Ana Carolina. Op. Cit., p. 166.

sem igual. Todavia, trata-se de um meio vulnerável à prática de atos ilícitos, até mesmo em decorrência da vasta gama de relações jurídico-sociais que nela se dão.

Havendo um conflito, será preciso efetuar uma ponderação de interesses, preservando-os o máximo. Necessariamente, um interesse cederá espaço ao outro para que ambos sejam exercidos, até mesmo por possuírem igual tratamento no ordenamento jurídico-constitucional. O excesso no exercício de tais direitos caracterizará ato ilícito, sujeito à tutela cível e à tutela penal.

Em que pese uma ilusão de que somente a tutela penal é eficaz para a reparação de atos ilícitos, o instituto da responsabilidade civil se mostra amplo o suficiente para resolver boa parte dos conflitos da *Web*, sem prejudicar o seu caráter libertário. A *Internet* clama por uma regulamentação tão dinâmica e flexível quanto ela mesma. Com efeito, será possível preservar a democracia digital, isto é, o exercício amplo da liberdade em todas as suas dimensões.

Não parece ser esta a posição adotada por uma parte do Poder Legislativo brasileiro, que atualmente delibera favoravelmente ao policalesco PL n. 84/1999, o qual contraria as diretrizes mundiais de aplicação do direito penal enquanto *ultima ratio*. As críticas ao projeto vão além da falta de técnica de certos dispositivos: esbarra em questões como falta de proporcionalidade e, principalmente, ausência de participação popular em sua discussão.

Por outro lado, o Marco Civil para a *Internet* (PL n. 2126/2011) desponta como uma postura legislativa mais liberal e democrática. Apesar de existirem questões técnicas do PL que merecem revisão, este tem o seu mérito por ter buscado na vontade dos internautas objeto para a formação de seu conteúdo.

Em suma, conclui-se que, por existirem limites inerentes ao exercício da liberdade, que se excedidos caracterizam atos ilícitos (expressão tomada *lato sensu*, envolvendo as esferas cível e penal), é impossível abrir mão da intervenção estatal. No entanto, o Estado deve intervir na *Internet* respeitando o máximo possível as suas peculiaridades, garantindo a preservação do caráter democrático e libertário. Tal postura pode ser tomada no Judiciário, ao decidir

com base na Nova Hermenêutica constitucional, e no Legislativo, criando espécies normativas que não engessem a rede, a exemplo do que seria o Marco Civil para a *Internet*.

A adoção de princípios diretores, da priorização da responsabilidade civil em detrimento da penal e do reforço das possibilidades hermenêuticas é fundamental para que se tenha uma efetiva democracia digital no Brasil. Cabe à atuação legislativa estatal optar por este rumo, impulsionada pelos debates a respeito da temática na *Internet*, que não devem cessar.

6 Referências

- ANDRADE NETO, João; SIQUEIRA, Gustavo Silveira. A revolução será tuitada: como a Internet pode estimular o exercício público das liberdades. In: XX Congresso Nacional do CONPEDI, 2011, Vitória/ ES. **Anais do XX Congresso Nacional do CONPEDI**. Florianópolis: Fundação Boiteux, 2011. p. 3440-3462.
- ARANHA, Maria Lúcia de Arruda; MARTINS, Maria Helena Pires. **Filosofando**: Introdução à Filosofia. 3 ed. São Paulo: Moderna, 2003.
- ARISTÓTELES. **Ética a Nicômaco**. Tradução Pietro Nassetti. São Paulo: Martin Claret, 2006.
- BELCHIOR, Luisa. Crimes na *internet* rendem mais que tráfico de drogas no Brasil, diz PF. **Folha on-line**, 20 maio 2008. Disponível em: <<http://www1.folha.uol.com.br/folha/informatica/ult124u403907.shtml>>. Acesso em: 15 nov. 2011.
- BRASIL. **Constituição da República Federativa do Brasil de 5 de outubro de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 10 fev. 2012.
- _____. **Lei n. 10406 de 10 de janeiro de 2002**. Código Civil. Disponível em: <<http://www.planalto.gov.br/ccivil/leis/2002/L10406.htm>>. Acesso em: 10 fev. 2012.
- _____. **Decreto-lei n. 2848 de 07 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 10 fev. 2012.
- _____. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para a Internet**, parte VIII: Códigos

- Maliciosos (*Malware*). Disponível em: <<http://cartilha.cert.br/download/cartilha-08-malware.pdf>>. Acesso em: 04 out. 2010.
- _____. Congresso Nacional. **Legislação**. Disponível em: <<http://www2.planalto.gov.br/presidencia/legislacao>>. Acesso em: 12 maio 2012.
- _____. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 84 de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 10 maio 2012.
- _____. Poder Legislativo. Câmara dos Deputados. **Parecer da Comissão de Constituição e Justiça no Projeto de Lei n. 84 de 24 de fevereiro de 1999**. Disponível em: <http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=15028>. Acesso em: 10 maio. 2012.
- _____. Poder Legislativo. Câmara dos Deputados. **Projeto de Lei n. 2.126 de 24 de agosto de 2011**. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetratamacao?idProposicao=517255>>. Acesso em: 10 maio 2012.
- CASTELLS, Manuel. **A Sociedade em Rede**. 9. ed. São Paulo: Paz e Terra, 2006. v. 1.
- CELLA, José Renato Gaziero. Reflexões filosóficas preliminares para o governo eletrônico e democracia digital. **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, n. 1, p. 49-54, jul./dez. 2009.
- COMUNIDADE DE CIBERCULTURA. **Pelo veto ao projeto de cibercrimes**: Em defesa da liberdade e do progresso do conhecimento na *Internet* Brasileira. Disponível em: <<http://www.petitiononline.com/veto2008/petition.html>>. Acesso em: 12 maio 2012.
- DAOUN, Alexandre Jean; BLUM, Renato M. S. Opice. Cybercrimes. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Coord.). **Direito & Internet**: Aspectos Jurídicos Relevantes. Bauru: Edipro, 2000. p. 117-129.
- DINIZ, Laura. Justiça Derruba Anonimato e Pune Cada Vez Mais por Crimes na *Internet*. **O Estado de São Paulo**. São Paulo, p. C1, 01 out. 2008.
- FERREIRA, Aurélio Buarque de Holanda. **Miniaurélio**: o minidicionário da língua portuguesa. Curitiba: Positivo, 2004.
- GANDELMAN, Henrique. **De Gutenberg à Internet**: Direitos Autorais das Origens à Era Digital. 5. ed. São Paulo: Record, 2007.

- GARCIA, Bruna Pinotti. **Ética na Internet**: os conflitos entre particulares no ciberespaço face às dimensões da liberdade e os princípios éticos como base de solução. 2010. 150 f. Trabalho de Curso (Bacharelado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino “Eurípides Soares da Rocha”, Marília, 2010.
- GONÇALVES, Carlos Roberto. **Responsabilidade Civil**. 9. ed. São Paulo: Saraiva, 2005.
- GUIMARÃES, José Augusto Chaves; FURLANETO NETO, Mário. Crimes na *Internet*: elementos para uma reflexão sobre a ética informacional. **Revista CEJ**, Brasília, v. 7, n. 20, p. 67-73, jan./mar. 2003.
- JESUS, Damásio Evangelista de. **Direito Penal**. 15. ed. São Paulo: Saraiva, 2003. v. 2.
- KANT, Immanuel. **Crítica da Razão Prática**. Tradução Paulo Barrera. São Paulo: Ícone, 2005.
- LÉVY, Pierre. **Cibercultura**. Tradução Carlos Irineu da Costa. 2. ed. São Paulo: Editora 34, 2003.
- LIMA, Gisele Truzzi de; DAOUN, Alexandre Jean. **Crimes Informáticos: o Direito Penal na Era da Informação**. Disponível em: <<http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf>>. Acesso em: 03 nov. 2009.
- MAIA, Rousiley C. M. **Democracia e a Internet como esfera pública virtual**: aproximando as condições do discurso e da deliberação. Disponível em: <<http://vsites.unb.br/fac/comunicacaoepolitica/Rousiley2001.pdf>>. Acesso em: 09 jun. 2012.
- MICROSOFT. **Phishing**: Perguntas Frequentes. Disponível em: <<http://www.microsoft.com/brasil/protect/yourself/phishing/faq.msp>>. Acesso em: 05 out. 2010.
- MOTTA, Sylvio; BARCHET, Gustavo. **Curso de Direito Constitucional**. Rio de Janeiro: Elsevier, 2007.
- OLIVO, Luís Carlos Cancellier de. Os “Novos” Direitos enquanto Direitos Públicos Virtuais na Sociedade da Informação. In: WOLKMER, Antônio Carlos; LEITE, José Rubens Morato (Org.). **Os “Novos” Direitos no Brasil**: Natureza e Perspectivas. São Paulo: Saraiva, 2003. p. 319-353.
- PAESANI, Liliana Minardi. **Direito de Informática: Comercialização e Desenvolvimento Internacional do Software**. 3. ed. São Paulo: Atlas, 2001.
- _____. **Direito e Internet**: Liberdade de Informação, Privacidade e Responsabilidade Civil. 3. ed. São Paulo: Atlas, 2006.
- PECK, Patrícia. **Direito Digital**. São Paulo: Saraiva, 2002.

- PINHEIRO, Patrícia Peck. **Uso Ético e Responsável da *Internet***: Dicas e Alertas. São Paulo: Fundação Bradesco, 2009.
- SANTOS, José Eduardo Lourenço dos. **Proteção da Privacidade na *Internet***: Aspectos Criminais. 2002. 129f. Dissertação (Mestrado em Direito) – Centro Universitário Eurípides de Marília, Fundação de Ensino “Eurípides Soares da Rocha”, Marília, 2002.
- SÃO PAULO. Tribunal de Justiça do Estado de São Paulo. **Apelação n. 9110832-40.2006.8.26.0000**. Relator: Elliot Akel. São Paulo, 20 de outubro de 2010. Disponível em: www.tj.sp.gov.br. Acesso em: 15 nov. 2011.
- SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25. ed. São Paulo: Malheiros, 2006.
- VAZ, Ana Carolina. Neutralidade da Rede, Proteção de Dados Pessoais e Marco Regulatório da *Internet* no Brasil. **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, n. 5, p. 147-171, jul./dez. 2011.
- VENOSA, Sílvio de Salvo. **Direito Civil: Responsabilidade Civil**. 6. ed. São Paulo: Atlas, 2006. v. 4.